

CLAIM AMENDMENTS

1 1. (currently amended) A method of preventing the loss
2 of confidentiality of electronically stored data in a computer
3 system [[[11, 12, 13]]], which data in particular is organized as a
4 data system [[[103]]] and or subdivided into blocks, in particular
5 with use of exchangeable and/or removable data carriers and/or
6 storage medium, where in particular peripherals are connectable to
7 the computer system [[[11, 12, 13]]], characterized by the
8 following steps:

9 analysis of the protocol and of the data stream [[[130,
10 131]]] from and to data carriers and/or storage media [[[104]]]
11 and/or peripheral devices;

12 establishment of a classification, in particular for
13 differentiation between nonremovable and removable data carriers
14 and/or storage media [[[104]]];

15 determination on the basis of the established
16 classification, whether an encryption of the electronically stored
17 data is required for preventing the loss of confidentiality of the
18 data and, depending on this determination, possibly

19 adding a cryptographic encryption [[[601, 602, 603]]] to
20 the data system on a removable data carrier and/or a removable
21 storage medium [[[104]]], [[and/]] or performing a cryptographic

22 encryption on all or several blocks of the removable data carrier
23 and/or of the removable storage medium $[(104)]$.

1 2. (currently amended) The method according to claim 1,
2 ~~characterized by , further comprising the step of~~
3 determining that an encryption $[(105)]$ of all blocks
4 of the data carrier/storage medium $[(104)]$ or an encryption
5 $[(105)]$ of all files $[(50)]$ before storage on the data
6 carrier/storage medium $[(104)]$ and that an encryption $[(105)]$
7 of several files $[(50)]$ before storage on the data carrier
8 /storage medium $[(104)]$ is carried out.

1 3. (currently amended) The method according to claim 1
2 ~~or 2, characterized in that wherein~~ a cryptographic encryption is
3 added to each data system $[(103)]$ on nonremovable $[[\text{and}/]]$ or
4 nonexchangeable data carriers $[[\text{and}/]]$ or storage media $[(104)]$.

1 4. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that claim 3 wherein~~ the
3 cryptographic encryption $[(105)]$ is temporarily suspended when
4 particular features are shown.

1 5. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein when a
3 data carrier ~~[[and/]]~~ or a storage medium ~~[[(104)]]~~ without data
4 system ~~[[are]]~~ is used, an encryption of all blocks is carried out
5 and access is prevented.

1 6. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein an
3 encryption ~~[[(105)]]~~ is performed when removable data carriers and
4 or removable storage media ~~(104), in particular floppy disks,~~
5 ~~memory sticks, CD-RW, DVD-RW and the like,~~ are used.

1 7. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein an
3 encryption ~~[[(105)]]~~ is performed when removable data carriers
4 ~~[[and/]]~~ or nonremovable storage media ~~[[(104)]]~~, ~~[[and/]]~~ or
5 network based data carriers ~~[[and/]]~~ or network based storage media
6 ~~[[(104)]]~~ are used.

1 8. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein when a
3 data carrier ~~[[and/]]~~ or a storage medium ~~[[(104)]]~~ is connected to
4 a multifunctional interface ~~[[and/]]~~ or a multifunctional bus, ~~in~~
5 ~~particular slot, USB-port, and the like,~~ the functionality of the
6 interfaces ~~[[and/]]~~ or the buses is maintained and an encryption

7 [[(105)]] is only performed on [[the]] data streams [[(130, 131)]]
8 that are further transmitted to the interface [[and/]] or the bus
9 for storing the data.

1 9. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1, further
3 comprising the steps of

4 performing an analysis of the interface [[and/]] or the
5 bus to which a data stream [[(130, 131)]]
6 shall be transmitted ~~is~~
7 performed and [[that]]

8 taking the analysis ~~is taken~~ into account for
9 establishing the classification on the basis of ~~criteria that can~~
10 ~~be determined, in particular on the basis~~ of the physical
11 connection [[and/]] or the properties of the devices.

1 10. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein
3 cryptographic methods for encryption are applied , ~~in particular~~
4 ~~the Rijndael algorithm.~~

1 11. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein the
3 encryption is performed in ~~several steps, in particular in that~~
4 after performing accordance with a first cryptographic method, the

5 ~~data encrypted by the first method and thereafter~~ is again
6 encrypted by means of a second cryptographic method.

1 12. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that claim 1, further~~
3 ~~comprising the step of~~, during a reading process from a data
4 carrier ~~[[and/]]~~ or storage medium ~~[(104)]~~ that is at least
5 partially encrypted,
6 performing a decryption of the data is performed.

1 13. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that claim 1, further~~
3 ~~comprising the step of~~
4 preventing encryption of the data by using hardware with
5 an integrated key [[and/]] or by using a password [[and/]] or by
6 recognizing and controlling biometric data of a user , an
7 ~~encryption (105) of data can be prevented.~~

1 14. (currently amended) The method according to claim
2 ~~13, characterized in that , further comprising the step of~~
3 preventing the encryption (105) can be prevented only at
4 predetermined times.

1 15. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein for the
3 encryption ~~[[(105)]]~~, keys ~~[[(300)]]~~ are used that are formed by
4 combination of different parts ~~[[(301, 302, 303)]]~~, whereby in
5 particular several computer systems ~~[[(11, 12, 13)]]~~ can be
6 combined in groups ~~[[(10)]]~~, the keys ~~[[(300)]]~~ of a group ~~[[(10)]]~~
7 of computer systems ~~[[(11, 12, 13)]]~~ having a common part ~~[[(301)]]~~
8 as well as a respective individual part ~~[[(302)]]~~.

1 16. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 15 wherein the
3 key ~~[[(300)]]~~ that is to be applied for the encryption and
4 decryption ~~[[(105)]]~~ can be determined ~~[[and/]]~~ or stored in a data
5 base for being requested ~~[[and/]]~~ or is integrated in a hardware
6 ~~[[and/]]~~ or is determined from biometric data of a user by using an
7 algorithm.

1 17. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein actions
3 that are performed by means of the computer system ~~(11, 12, 13),~~
4 ~~such as storing and/or reading of data,~~ are recorded.

1 18. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein the
3 computer system $[(11, 12, 13)]$ has an operating system that at
4 least distinguishes between a kernel mode $[(100)]$ and a user mode
5 $[(200)]$, the method being at least partially implemented in the
6 kernel mode $[(100)]$.

1 19. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein a logic
3 combination of several computer systems $[(11, 12, 13)]$ within a
4 group $[(10)]$ is performed, wherein within the group $[(10)]$ the
5 cryptographic encryption $[(105)]$ is mutually suspended, wherein
6 the cryptographic encryption $[(105)]$ is maintained with respect
7 to external sources.

1 20. (currently amended) The method according to ~~one of~~
2 ~~the preceding claims, characterized in that~~ claim 1 wherein during
3 access on a data carrier $[\text{and/}]$ or storage medium $[(104)]$, it
4 is determined whether an encryption $[(105)]$ of all blocks of the
5 data carrier/storage medium $[(104)]$ or an encryption $[(105)]$ of
6 all files $[(50)]$ on the data carrier/storage medium $[(104)]$ or
7 an encryption $[(105)]$ of several files $[(50)]$ is present, and
8 that an encryption of the requested data is performed.